user manual

mobily... my world, my choice

customer service: 056-010-1100 | www.mobily.com.sa

موبايلي
mobily

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be broken or malfunctioning, please contact technical support for immediate service by email at technicalsupport@netcomm.com.au

For product updates, new product release, manual revision, or software upgrades, please visit our website at www.netcomm.com.au

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

WARNING

- Disconnect the power line from the device before servicing.

Copyright

Copyright©2010 NetComm Limited. All rights reserved. The information contained herein is proprietary to NetComm Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Limited

NOTE:This document is subject to change without notice.

Save Our Environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Table of Contents

2 Introduction 5
2.1 Features 5
2.2 Package Contents 5
2.3 LED Indicators 6
2.4 Panels 7

3. Quick Setup 9
3.1 Setup Procedure 9

4. Default Settings 11
4.1 Restore Factory Default Settings 11
4.2 WEB USER INTERFACE 12

6. 3G Settings 16
6.1 Setup 16
6.2 Signal Selection 16
6.3 PIN Configuration 16

7. WIFI 20
7.1 Setup 20
7.2 Security 21
7.3 Configuration 22
7.4 MAC Filter 24
7.5 Wireless Bridge 25
7.6 Station Info 25

8. Management 27
8.1 Device Settings 27
8.2 SNMP 28
8.3 SNTP 29
8.4 Access Control 29
8.5 Save/Reboot 30

9 Advanced Settings 32
9.1 LAN 32
9.2 NAT 33
9.3 Security 35
9.4 Parental Control 37
9.5 Routing 38
9.6 DNS 39
9.7 Print Server 40
9.8 USB Storage 40

10 Status 42
10.1 Diagnostics 42
10.2 System Log 43
10.3 3G Network 44
10.4 Statistics 45
10.5 Route 46
10.6 ARP 46
10.7 DHCP 46
10.8 PING 46

11 Appendix A: Print Server 48
11.1 For Windows Vista/7 48
11.2 For MAC OSX 50

12 Appendix B: Samba Server 51
12.1 For Windows Vista/7 51
12.2 For MAC OSX 51

Introduction

2 Introduction

Designed to keep up with the world's fastest networks, this DC-HSPA+ device is capable of downlink speeds of up to 42Mbps. With wireless N, this device also provides multiple wireless devices with local wireless speeds of up to 300Mbps. Its stylish vertical design incorporates a unique cable management design hiding up to 5 cables.

2.1 Features

- Combines DC-HSPA+, Wireless 11n 300Mbps, 4 Ethernet ports
- Worldwide coverage through Quad-band HSUPA/HSDPA/UMTS (850 / 900 / 1900 / 2100 Mhz), quad-band EDGE/GSM (850 / 900 / 1800 / 1900 Mhz)
- Integrated 802.11n AP (backward compatible with 802.11b/g)
- UPnP
- WEP/WPA/WPA2 and 802.1x
- MAC address and IP filtering
- Static route functions
- DNS Proxy
- NAT/PAT
- Embedded Sierra Wireless MC8801 multimode HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM module
- CLI command interface
- 2 x USB ports (for Print server functionality or accessing USB Storage)

2.2 Package Contents

Your package contains the following:

- Mobily Connect Router
- Printed Quick Start Guide
- CD (Containing User Guide)
- Ethernet Cable
- Wireless Security Card
- Power Supply
- Warranty sheet

2.3 LED Indicators

The LED indicators are explained in the table below.

LED	Icon	Color	Mode	Function
High		Blue	On	High signal strength
			Off	No activity, Router powered off or on other signal strength
Med		Blue	On	Medium signal strength
			Off	No activity. The Router is powered off or is currently using another signal strength
Low		Blue	On	Low signal strength
			Off	No activity. The Router is powered off or is currently using another signal strength
3G		Blue	On	Connection established with the 3G network
			Off	Either there is no activity or the Router is powered off
			Blink	Connecting with 3G network
2G		Blue	On	Connection established with the 2G network
			Off	Either there is no activity or the Router is powered off
			Blink	Connecting with 2G network
LAN 1-4		Blue	On	Powered device connected to the associated LAN port (includes devices with Wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection)
			Off	No device connected or Connected device is off
			Blink	LAN activity present (traffic in either direction)
Internet		Blue	On	Internet connection established
			Off	No connection to the internet or Router powered off
			Blink	Data is currently being transmitted through the Internet connection
Wi-Fi		Blue	On	Local Wi-Fi access to the Router is enabled and working
			Off	Local Wi-Fi access to the Router is disabled
			Blink	Data being transmitted or received over Wi-Fi.
Power		Blue	On	Power on
			Off	Power off

2.4 Panels

The rear and side panels shown below contain the ports for data and power connections.

1. USIM card slot
2. Four RJ-45 Ethernet LAN ports
3. Reset button
4. Power jack for DC power input (12VDC / 1.5A).
5. External 3G SMA Connector (Optional)
6. USB printer/hard drive
7. USB printer/hard drive

Quick Setup

3. Quick Setup

3.1 Setup Procedure

These steps explain how to quickly setup your Connect Router:

1. Insert your SIM card (until you hear a click) into the USIM slot on the rear of the Router.
2. Connect the yellow Ethernet cable to one of the yellow LAN ports found at the back of the Router.
3. Connect the other end of the yellow networking cable to the Ethernet port on your computer.
4. Connect the power adapter to the Power socket on the back of the Router.
5. Plug the power adapter into a wall socket and press the power button into the ON position.
6. Configure the Router through the Web User Interface (WUI).
7. Save the Router configuration and reboot .

Default Settings

4. Default Settings

LAN (Management)

Static IP Address: 192.168.1.X

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

WAN (Internet)

WAN mode: DHCP

Wireless

SSID: Refer to your wireless security card

Channel: Auto

Security: WPA-PSK

WEP Key: Refer to your wireless security card

Interface Access

Username: admin

Password: admin

4.1 Restore Factory Default Settings

Restoring factory defaults will reset the Connect Router to its factory default configuration. Occasions may present themselves where you need to restore the factory defaults on your Connect Router such as:

- You have lost your username and password and are unable to login to the web configuration page;
- You have purchased your Connect Router from someone else and need to reconfigure the device to work with your Mobily service;
- You are asked to perform a factory reset by support staff.

In order to restore your Connect Router to its factory default settings, please follow these steps:

- Ensure that your Connect Router is powered on (for at least 10 seconds);
- Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit at this point;
- When the indicator lights return to steady blue, the reset is complete. The default settings are now restored. The entire process takes about 45 seconds to complete;
- Once you have reset your Connect Router to its default settings you will be able to access the device's configuration web interface using http://192.168.1.1 with username 'admin' and password 'admin';

4.2 WEB USER INTERFACE

What can you do from here?

By logging into the web user interface, you are able to configure your Connect Router with a wide array of basic and advanced settings. From setting wireless security, to backing up your routers settings, uploading new firmware and setting parental controls, the web user interface is a handy tool for personalizing your device to maximize its potential. Read on for a more advanced description on all elements of the web user interface.

Logging into the web user interface

To login to the web user interface, follow the steps below:

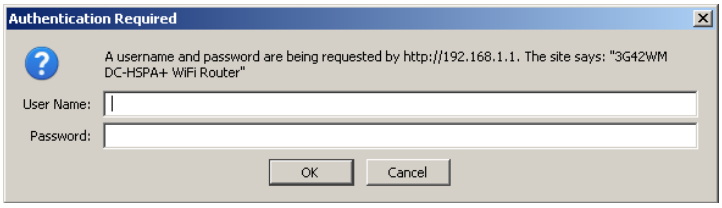
NOTE: The default settings can be found in section 4 - Default Settings.

1. Open a web browser and enter the default IP address for the Router in the web address field. In this case http://192.168.1.1

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet port of the router though not necessarily directly to the device. For remote access, use the WAN IP address shown on the WUI Homepage screen and login with remote username and password.

2. A dialog box will appear, as illustrated below. Enter the default username and password of admin.

Click OK to continue.



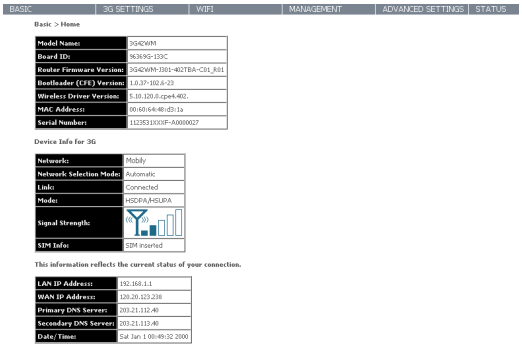
User Name – admin

Password – admin

NOTE: The login password can be changed later (see Access Control > Passwords)

BASIC

5. Basic - Home



The web user interface (WUI) is divided into two window panels, the main menu (on the top) and the display screen (on the bottom). The main menu has the following options: Basic, 3G Settings, Wi-Fi, Management, Advanced and Status.

Selecting one of these options will open a submenu with more options. Basic is discussed below while subsequent chapters introduce the other main menu selections.

NOTE: The menu options available within the web user interface are based upon the device configuration and user privileges (i.e. local or remote).

The following table provides further details

Field	Description
Model Name	Model number of your device
Board ID	The unique number of the board inside your device
Bootloader (CFE) Version	The version of the bootloader
Wireless Driver Version	The current version of wireless driver being used by your device
MAC Address	The MAC address of the network interface
Serial Number	The serial number of the unit
Device Info For 3G	
Network	The name of your 3G network
Link	The status of your 3G connection
Mode	The radio access technique currently used to enable internet access. It can be HSUPA, HSDPA, UMTS, EDGE, GPRS or Disconnected.
Signal Strength	The mobile network (UMTS) signal quality available at the device location. This signal quality affects the performance of the unit. If two or more bars are green, the connection is usually acceptable.
SIM Info	Shows the SIM card status on the device.
Connection Status	
LAN IP Address	Shows the IP address for LAN interface.
WAN IP Address	Shows the IP address for WAN interface.
Primary DNS Server	Shows the IP address of the primary DNS server.
Secondary DNS Server	Shows the IP address of the secondary DNS server.
Date/Time	The time according to the device's internal clock

3G Settings

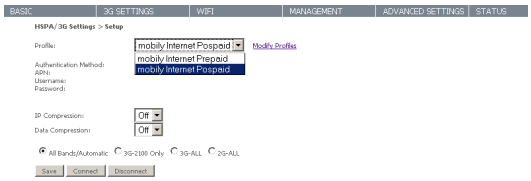
6. 3G Settings

6.1 Setup

This page allows you to select your 3G service settings according to predefined or custom profiles. Setup instructions are provided in the following sections for your assistance.

Your 3G Service Provider will provide the information required to complete the first time setup instructions below. This includes profile, username and password. Only complete those steps for which you have information and skip the others.

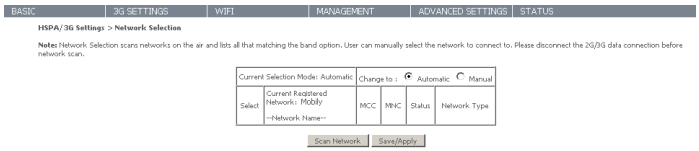
1. If your SIM card is not inserted into the Router, then do so now.
2. Select the appropriate 3G Settings Profile. You can select either mobily Prepaid or mobily Postpaid. Alternatively, enter a custom connection profile by clicking on the “Modify Profiles” link, then click the “Add” button and enter the details supplied by your 3G provider.



3. Select to turn IP compression and Data compression to be On or Off. If you are unsure or have no preference, leave it as the default value.
4. Enter the MTU rate. If you are unsure or have no preference, leave it as the default value
5. Click the Save button to save the new settings.
6. Press the Connect button to connect to Internet. The Device Info for the 3G network status box in the WUI Basic screen should indicate an active connection.

6.2 Signal Selection

By default, a stable signal is obtained from the antennas built into the Connect Router. To use an external 3G antenna, please connect it to the Antenna Connector next to the Power Input on the back of the router. The router will automatically use the external antenna connector when an external antenna is connected to it.



6.3 PIN Configuration

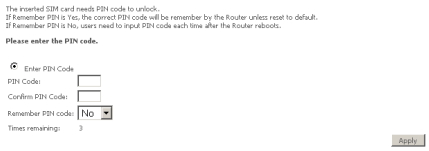
This screen allows for changes to the 3G SIM card PIN code protection settings.

NOTE: If you have entered the incorrect PIN 3 times, your SIM card will be locked for your security. Please call Mobily for assistance.

6.3.1 PIN Code Protection

PIN code protection prevents the use of a SIM card by unauthorized persons. To use the 3G internet service with this router however, the PIN code protection should be disabled. If the SIM card inserted into the router is locked with a PIN code, the web user interface will display the following screen after first login.

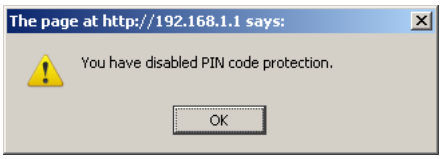
Please input the PIN code, select Remember PIN code as Yes and click Apply.


The inserted SIM card needs PIN code to unlock.
If Remember PIN is Yes, the correct PIN code will be remember by the Router unless reset to default.
If Remember PIN is No, users need to input PIN code each time after the Router reboots.
Please enter the PIN code.
Enter PIN Code
PIN Code:
Confirm PIN Code:
Remember PIN code: No
Times remaining: 3
Apply

PIN Lock Off

If you wish to always connect to the Internet using a PIN locked SIM card, you should first turn PIN code protection off. Please click on PIN Configuration from the menu.

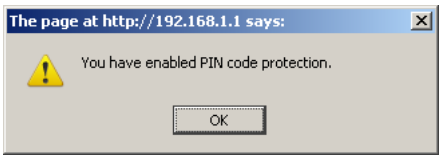
Select Change PIN Code Protection. Un-tick Enable PIN Lock and enter the PIN code twice. Please keep in mind you only have 3 attempts before your SIM card is locked. The Times remaining shows how many attempts are left. Contact Mobily if you require assistance. Afterwards, click Apply. The following dialog box should now appear.



PIN Lock On

After you are finished using your SIM card for Internet access, you may wish to lock the SIM card again. In this case, first go to the PIN configuration screen, as shown below.

Select Change PIN Code Protection. Tick Enable PIN Lock, enter the PIN code twice. You can set Remember PIN code to yes so you don't need to input the PIN code every time when the gateway turns on with this SIM inserted. Then click Apply. After you do so, the following dialog box should appear.

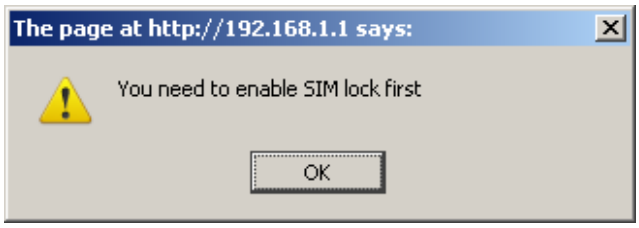


You can now return your SIM card to your cellular phone or other mobile device.

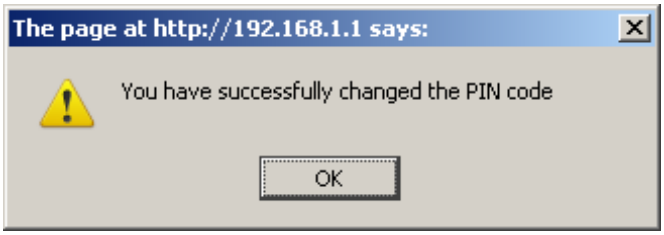
6.3.2 PIN Code Change

If you wish to change your PIN code for greater security, go to the previous section and follow the procedure listed under PIN Lock On. After locking the SIM card, select PIN Code Change and enter your old and new PIN codes in the fields provided. Keep in mind you only have 3 attempts before your SIM card is locked. The Times remaining shows how many attempts left. Contact Mobily if you require assistance. Afterwards, click apply to activate the change.

If you forget to turn on PIN lock protection before changing your PIN, you will see this dialog box as a helpful reminder.



If your PIN code change request was successful the following dialog box will display.



WIFI

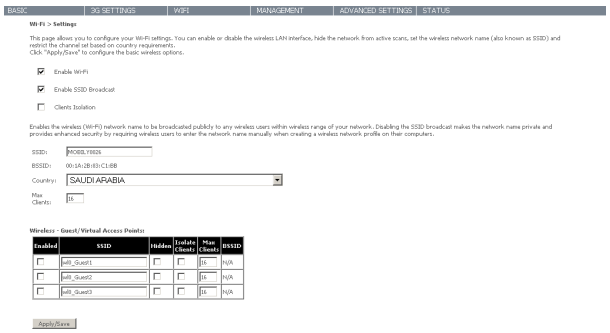
7. WIFI

7.1 Setup

The WiFi submenu provides access to the Wireless Local Area Network (WLAN) configuration settings including:

- Wireless network name (SSID)
- Channel restrictions (based on country)
- Security
- Access point or bridging behaviour
- Station information

This screen allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as the SSID) and restrict the channel set based on country requirements. The Wireless Guest Network function adds extra networking security when connecting to remote hosts.



Option	Description
Enable WiFi	A checkbox that enables or disables the wireless LAN interface. The default is Enable WiFi.
Enable SSID Broadcast	Deselect Enable SSID Broadcast to protect the access point from detection by wireless network scans. To check AP status in Windows XP, open Network Connections from the Start Menu and select View Available Network Connections. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood. 2. Prevents one wireless client communicating with another wireless client.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum number of characters: 1, maximum number of characters: 32.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range.
Wireless Guest Network	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the radio buttons under the Enable heading. To hide a Guest SSID, select its radio button under the Hidden heading. Do the same for Isolate Client. For a description of this function, see the entry for "Client Isolation" in this table. Similarly, for Max Clients and BSSID headings, consult the matching entries in this table. NOTE: Remote wireless hosts are unable to scan Guest SSIDs.

7.2 Security

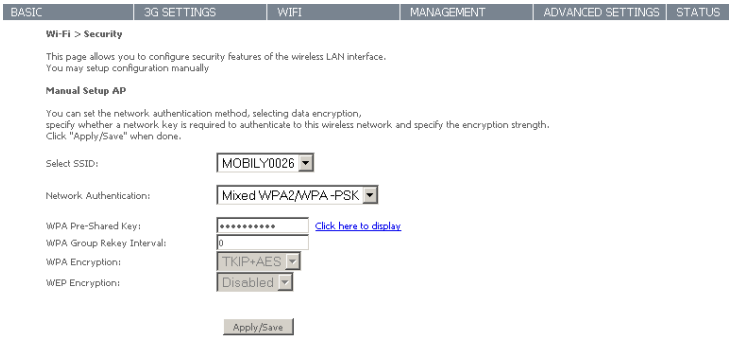
This router includes a number of options to help provide a secure connection to the Wi-Fi Network.

Security features include:

- WEP / WPA / WPA2 data encryption
- MAC address IP filtering

You can authenticate or encrypt your service on the Wi-Fi Protected Access algorithm, which provides protection against unauthorized access such as eavesdropping.

The following screen appears when Security is selected. The Security page allows you to configure security features of your router's WLAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.



Click Apply/Save to configure the wireless security options.

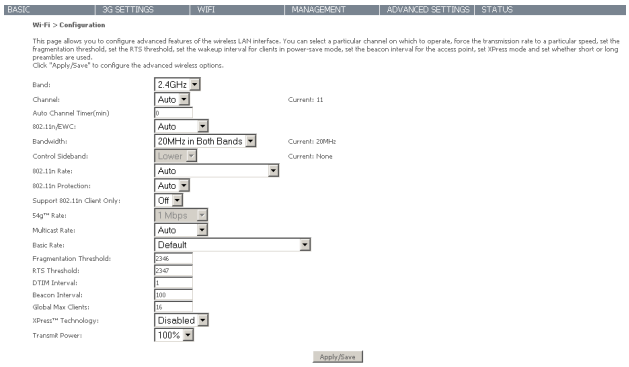
Option	Description
Select SSID	The Connect router is able to handle multiple wireless networks. The pull down menu enables you to select which wireless network the security settings will be applied to.
Network Authentication	This option is used for authentication to the wireless network. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and key fields.
WEP Encryption	This option indicates whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Whilst four network keys can be defined, only one can be used at any one time.
WPA-PSK / WPA2-PSK	A new type of wireless security that gives a more secure network when compared to WEP. The security key needs to be more than 8 characters and less than 63 characters and it can be any combination of letters and numbers. This is the default wireless security in use on the router. Default value is listed on your security card
WPA	WPA (Wi-Fi Protected Access) is suitable for enterprise applications. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management.
Encryption Strength	The strength/length of your wireless security key.
Current Network Key	The current network key that is active. You have the choice of setting up to 4 different wireless security keys
Network Key 1	The value of network key 1.
Network Key 2	The value of network key 2
Network Key 3	The value of network key 3
Network key 4	The value of network key 4

7.3 Configuration

This screen allows you to control the following advanced features of the Wireless Local Area Network (WLAN) interface:

- Select the channel which you wish to operate from
- Force the transmission rate to a particular speed
- Set the fragmentation threshold
- Set the RTS threshold
- Set the wake-up interval for clients in power-save mode
- Set the beacon interval for the access point
- Set XpressTM mode
- Program short or long preambles

Click Apply/Save to set the advanced wireless configuration.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Wi-Fi > Configuration
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wake-up interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply/Save" to configure the advanced wireless options.
Band: 2.4GHz
Channel: Auto Current: 11
Auto Channel Timer(min) 0
802.11n/EWC: Auto
Bandwidth: 20MHz in Both Bands Current: 20MHz
Control Sideband: Lower Current: None
802.11n Rate: Auto
802.11n Protection: Auto
Support 802.11n Client Only: Off
54g™ Rate: 1 Mbps
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 16
XPress™ Technology: Disabled
Transmit Power: 100%
Apply/Save

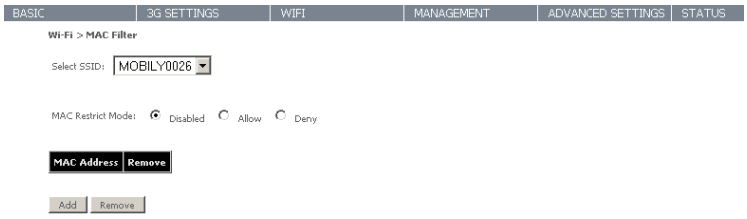
Option	Description
Band	The frequency of the wireless network. 2.4GHz is standard.
Channel	Allows selection of a specific channel (1-14) or Auto mode.
Auto Channel Timer	The Auto Channel times the length it takes to scan in minutes.
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	The drop-down menu specifies the following bandwidth: 20MHz in 2.4G Band and 40 MHz in 5G Band, 20MHz in both bands and 40MHz in both bands
Control Sideband	This is available for 40MHz. Drop-down menu allows selecting upper sideband or lower sideband
802.11n Rate	Drop-down menu specifies the following fixed rates. The maximum rate for bandwidth, 20MHz, is 130Mbps and the maximum bandwidth, 40MHz, is 270Mbps
802.11n Protection	Turn off for maximized throughput Turn on for greater security
Support 802.11n Client Only	The option to provide wireless Internet access only to clients who are operating at 802.11n speeds
54g Rate	In Auto (default) mode, your Router uses the maximum data rate and lowers the data rate dependent on the signal strength. The appropriate setting is dependent on signal strength. Other rates are discrete values between 1 to 54 Mbps.
Multicast rate	Setting for multicast packet transmission rate. (1-54 Mbps)
Basic Rate	Sets basic transmission rate.
Fragment Threshold	A threshold (in bytes) determines whether packets will be fragmented and at what size. Packets that exceed the fragmentation threshold of an 802.11 WLAN will be split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value however are not fragmented. Values between 256 and 2346 can be entered but should remain at a default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request To Send (RTS) specifies the packet size that exceeds the specified RTS threshold, which then triggers the RTS/CTS mechanism. Smaller packets are sent without using RTS/CTS. The default setting of 2347 (max length) will disables the RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in is milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon.
Global Max Clients	Here you have the option of setting the limit of the number of clients who can connect to your wireless network
Xpress Technology	Broadcom's Xpress™ Technology is compliant with draft specifications of two planned wireless industry standards. It has been designed to improve wireless network efficiency. Default is disabled
Transmit Power	The option of decreasing the transmitting power of your wireless signal

7.4 MAC Filter

This screen appears when Media Access Control (MAC) Filter is selected. This option allows access to be restricted based upon the unique 48-bit MAC address.

To add a MAC Address filter, click the Add button shown below.

To delete a filter, select it from the table below and click the Remove button.



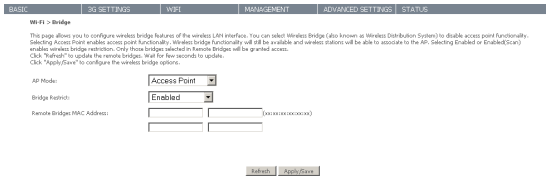
Option	Description
MAC Restrict Mode	Disabled – Disables MAC filtering Allow – Permits access for the specified MAC addresses. NOTE: Add a wireless device's MAC address before clicking the Allow radio button or else you will need to connect to the Router's web user interface using the supplied yellow Ethernet cable and add the wireless device's MAC address. Deny – Rejects access for the specified MAC addresses
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. A maximum of 60 MAC addresses can be added.

Enter the MAC address on the screen below and click Apply/Save.

7.5 Wireless Bridge

The following screen appears when selecting Wireless Bridge, and goes into a detailed explanation of how to configure wireless bridge features of the wireless LAN interface.

Click Apply/Save to implement new configuration settings.

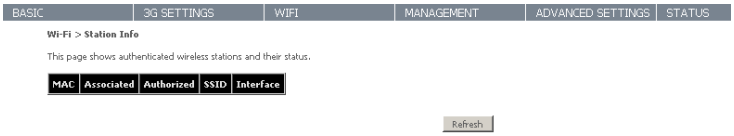


Option	Description
AP Mode	Selecting Wireless Bridge (Wireless Distribution System) disables Access Point (AP) functionality while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled in Bridge Restrict disables Wireless Bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) allows wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

7.6 Station Info

The following screen appears when you select Station Info, and shows authenticated wireless stations and their status.

Click the Refresh button to update the list of stations in the WLAN.



Option	Description
MAC	The MAC address of any connected client
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	The SSID of your wireless network
Interface	The wireless interface being used to connect

Management

8. Management

8.1 Device Settings

The Device Settings screens allow you to backup, retrieve and restore the default settings of your Router. It also provides a function for you to update your Routers firmware.

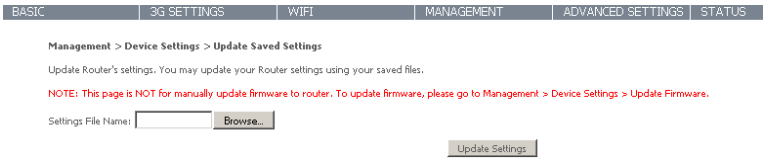
8.1.1 Backup

The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings.

You will be prompted to choose the location on your PC to save the backed up configuration file to.

8.1.2 Update

The following screen appears when selecting Update from the submenu. By clicking on the Browse button, you can locate a previously saved backup configuration file as the configuration backup file to use to update your Connect routers configuration. Click on the Update settings to load it.

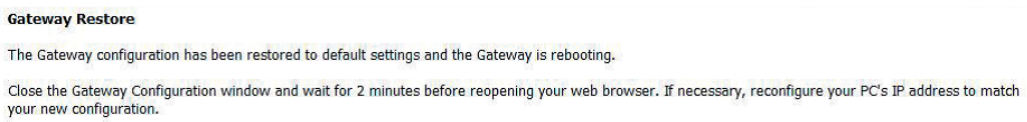

BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Management > Device Settings > Update Saved Settings
Update Router's settings. You may update your Router settings using your saved files.
NOTE: This page is NOT for manually update firmware to router. To update firmware, please go to Management > Device Settings > Update Firmware.
Settings File Name:
Browse...
Update Settings

8.1.3 Restore Default

The following screen appears when selecting Restore Default. By clicking on the Restore Default Settings button, you can restore your Routers default firmware settings. To restore system settings, reboot your Router.

NOTE: The default settings can be found in section 4 Default Settings.

Once you have selected the Restore Default Settings button, the following screen will appear. Close the window and wait 2 minutes before reopening your browser. If required, reconfigure your PCs IP address to match your new configuration

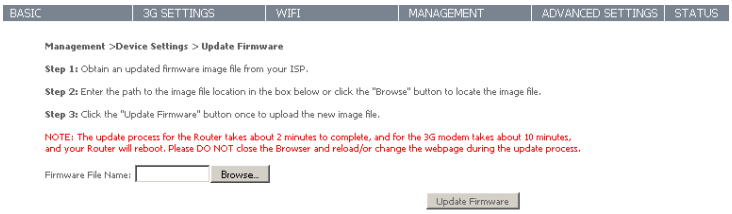

Gateway Restore
The Gateway configuration has been restored to default settings and the Gateway is rebooting.
Close the Gateway Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

After a successful reboot, the browser will return to the Device Info screen. If the browser does not refresh to the default screen, close and restart the browser and then enter http://192.168.1.1 into the address bar at the top of your browser window.

NOTE: The Restore Default function has the same effect as the reset button. The device board hardware and the boot loader support the reset to default button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

8.1.4 Update Firmware

The following screen appears when selecting Update Firmware. By following this screens steps, you can update your Routers firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

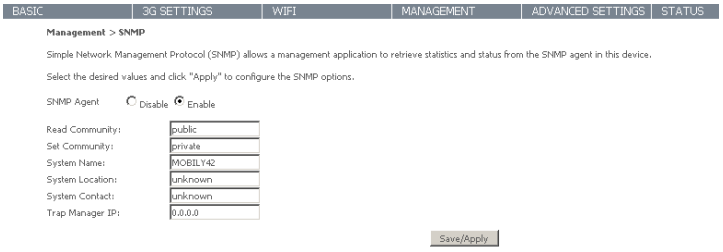

BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Management >Device Settings > Update Firmware
Step 1: Obtain an updated firmware image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Firmware" button once to upload the new image file.
NOTE: The update process for the Router takes about 2 minutes to complete, and for the 3G modem takes about 10 minutes, and your Router will reboot. Please DO NOT close the Browser and reload/or change the webpage during the update process.
Firmware File Name:
Browse...
Update Firmware

1. Obtain an updated software image file
2. Enter the path and filename of the firmware image file in the Software File Name field or click the Browse button to locate the image file.
3. Click the Update Software button once to upload and install the file.

NOTE: The update process will take about 2 minutes to complete. The Router will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the Software Version at the top of the Basic screen (WUI homepage) with the firmware version installed, to confirm the installation was successful.

8.2 SNMP

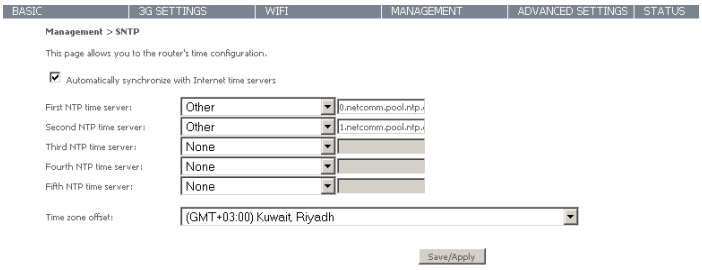
The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the 3G42W-M (if SNMP enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.



Option	Description
Read Community	Read device settings
Set Community	Read and change device settings
System Name	Default = Mobily42
System Location	User defined value
System Contact	User defined value
Trap Manager IP	IP address of admin machine

8.3 SNTP

This screen allows you to configure the time settings of your Router.



Option	Description
First NTP timeserver:	Select the required server.
Second NTP timeserver:	Select second timeserver, if required.
Time zone offset:	Select the local time zone.

NOTE: SNTP must be activated to use Parental Control.

8.4 Access Control

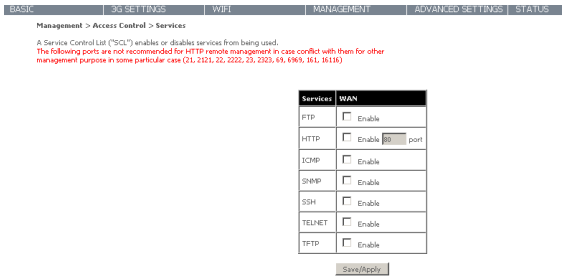
The Access Control option found in the Management drop down menu configures access related parameters in the following three areas:

- Services
- Passwords
- Save/Reboot

Access Control is used to control local and remote management settings for your Router.

8.4.1 Services

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP. Click Apply/ Save to continue.

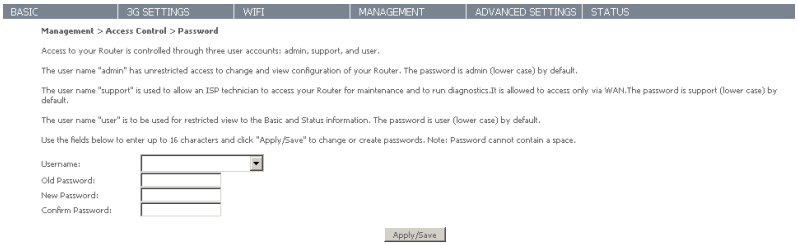


8.4.2 Passwords

The Passwords option configures your Web UI account access password for your Router. Access to the device is limited to the following three user accounts:

- admin is to be used for local unrestricted access control
- support is to be used for remote maintenance of the device
- user is to be used to view information and update device firmware

Use the fields illustrated in the screen below to change or create your password. Passwords must be 16 characters or less with no spaces. Click Apply/Save to continue.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Management > Access Control > Password
Access to your Router is controlled through three user accounts: admin, support, and user.
The user name "admin" has unrestricted access to change and view configuration of your Router. The password is admin (lower case) by default.
The user name "support" is used to allow an ISP technician to access your Router for maintenance and to run diagnostics.It is allowed to access only via WAN.The password is support (lower case) by default.
The user name "user" is to be used for restricted view to the Basic and Status information. The password is user (lower case) by default.
Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.
Username:
Old Password:
New Password:
Confirm Password:
Apply/Save

8.5 Save/Reboot

This function saves the current configuration settings and reboots your Router.

NOTE 1: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings.

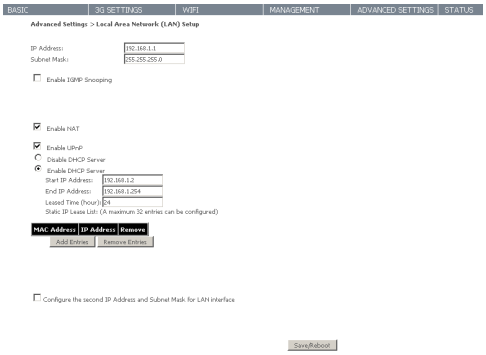
NOTE 2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore default settings.

Advanced Settings

9 Advanced Settings

9.1 LAN

This screen allows you to configure the Local Area Network (LAN) interface on your Router.



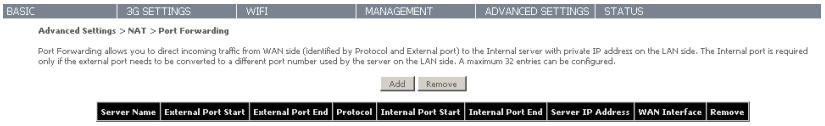
See the field descriptions below for more details.

Option	Description
IP Address	Enter the IP address for the LAN interface
Subnet Mask	Enter the subnet mask for the LAN interface
Enable IGMP Snooping	Enable by ticking the box Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group. Blocking Mode: In blocking mode, the multicast data traffic will be blocked. When there are no client subscriptions to a multicast group, it will not flood to the bridge ports.
Enable LAN side Firewall	Check box to enable Firewall on LAN
Disable DHCP Server	Disables the DHCP server. Only to be done if Static IP address is set up
Enable DHCP Server	Select Enable DHCP server and enter your starting and ending IP addresses and the lease time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every DHCP client on your LAN
Enable DHCP Server Relay	To relay DHCP requests from the subnet with no DHCP server on it to a DHCP server on other subnets. DHCP Server Relay is disabled by default. To access enable DHCP relay, please un-tick NAT enable first, that means to disable NAT first, and then press save button.
Configure the second IP Address and Subnet Mask for LAN Interface	Configure a second IP address by ticking the checkbox shown below and enter the following information: Enter the secondary IP address for the LAN interface. Enter the secondary subnet mask for the LAN interface.

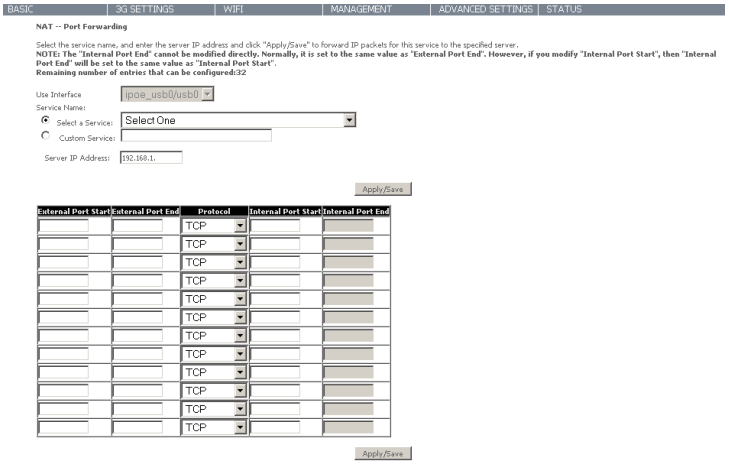
9.2 NAT

9.2.1 Port Forwarding

Port Forwarding allows you to direct incoming traffic from the Internet side (identified by Protocol and External port) to the internal server with a private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Settings > NAT > Port Forwarding
Port Forwarding allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.
Add
Remove
Server Name
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
Server IP Address
WAN Interface
Remove

To add a Virtual Server, click the Add button. The following screen will display.

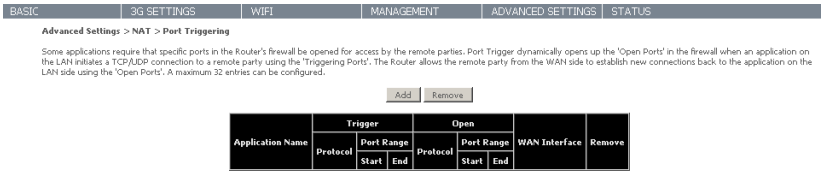

BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
NAT -- Port Forwarding
Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
Remaining number of entries that can be configured:32
Use Interface
Service Name:
Select a Service:
Select One
Custom Service:
Server IP Address:
192.168.1.
Apply/Save
External Port Start
External Port End
Protocol
Internal Port Start
Internal Port End
TCP
Apply/Save

Option	Description
Select a Service or Custom Server	User should select the service from the list. Or create a custom server and enter a name for the server
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

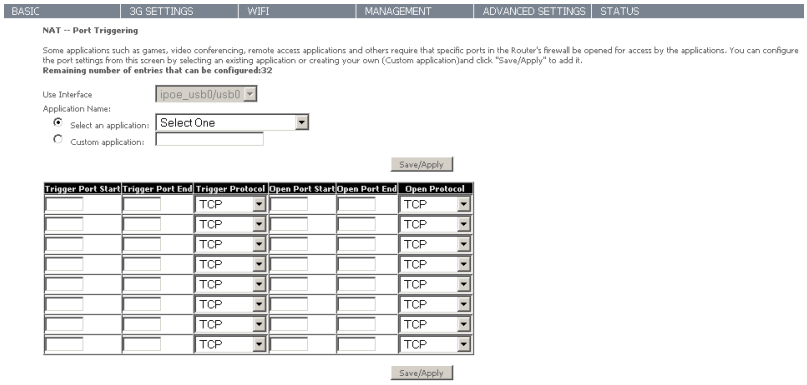
9.2.2 Port Triggering

Some applications require specific ports in the Router's firewall to be open for access by remote parties. Port Triggering opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'.

The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Settings > NAT > Port Triggering
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.
Add
Remove
Application Name
Trigger
Open
Protocol
Port Range
Start
End
WAN Interface
Remove

To add a Trigger Port, simply click the Add button. The following will be displayed.

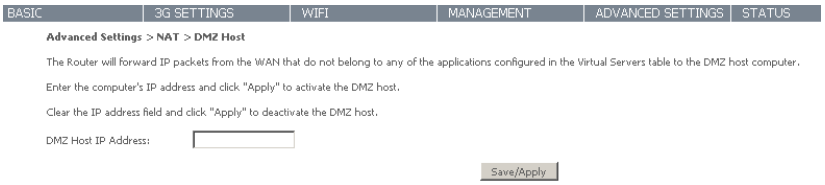

BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
NAT -- Port Triggering
Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.
Remaining number of entries that can be configured:32
Use Interface
ipoe_usb0/usb0
Application Name:
Select an application:
Select One
Custom application:
Save/Apply
Trigger Port Start
Trigger Port End
Trigger Protocol
Open Port Start
Open Port End
Open Protocol
TCP
Save/Apply

Option	Description
Select an Application or Custom Application	User should select the application from the list. Or the user can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP or UDP

9.2.3 DMZ Host

Your Router will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click Apply to activate the DMZ host. Clear the IP address field and click Save/Apply to deactivate the DMZ host.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Settings > NAT > DMZ Host
The Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.
DMZ Host IP Address:
Save/Apply

9.3 Security

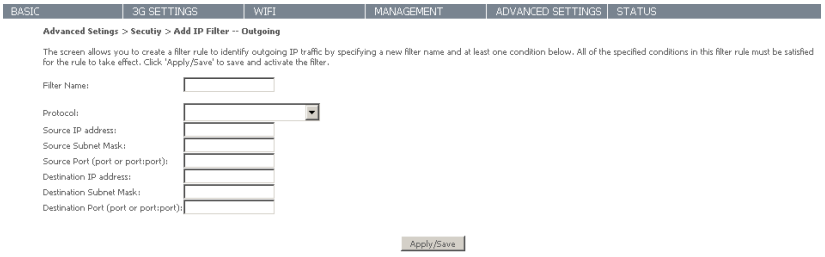
9.3.1 IP Filtering

The IP Filtering screen sets filter rules that limit incoming and outgoing IP traffic. Multiple filter rules can be set with at least one limiting condition. All conditions must be fulfilled before individual IP packets can pass the filter.

Outgoing IP Filter

The default setting for Outgoing traffic is ACCEPTED. Under this condition, all outgoing IP packets that match the filter rules will be BLOCKED.

To add a filtering rule, click the Add button. The following screen will display.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Setings > Secutiy > Add IP Filter -- Outgoing
The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Filter Name:
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
Apply/Save

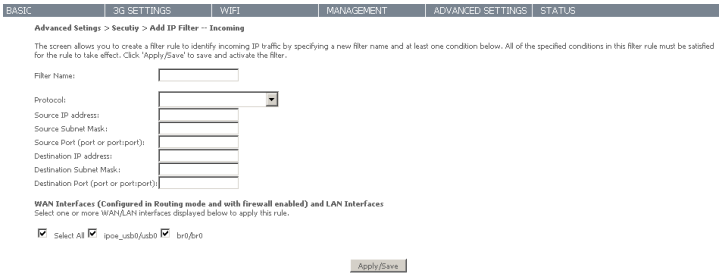
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP or ICMP Source IP address
Source IP address	Enter source IP address Source Subnet Mask
Destination IP address	Enter source subnet mask
Source Port (port or port:port)	Enter source port number or port range
Destination IP address	Enter destination IP address
Destination Subnet Mask	Destination Subnet Mask
Destination port (port or port:port)	Enter destination port number or range

Click Apply/Save to save and activate the filter.

Incoming IP Filter

The default setting for all Incoming traffic is BLOCKED. Under this condition only those incoming IP packets that match the filter rules will be ACCEPTED.

To add a filtering rule, click the Add button. The following screen will display.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Setings > Securiy > Add IP Filter -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Filter Name:
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.
Select All
ipoe_usb0/usb0
br0/br0
Apply/Save

Please refer to the Outgoing IP Filter table for field descriptions.

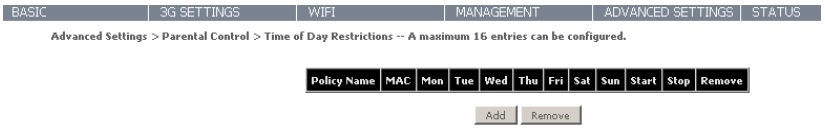
Click Apply/Save to save and activate the filter.

9.4 Parental Control

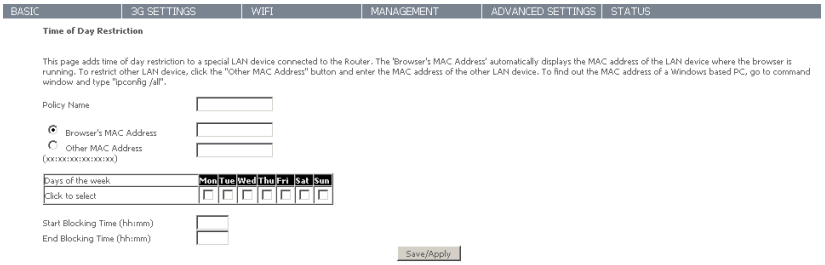
The Parental Control feature allows you to take advanced measures to ensure the computers connected to the LAN are used only when and how you decide.

9.4.1 Time Restriction

This Parental Control allows you to restrict access from a Local Area Network (LAN) to an outside network through the Router on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.3 SNTP, so that the scheduled times match your local time.



Click Add to display the following screen.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Time of Day Restriction
This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".
Policy Name
Browser's MAC Address
Other MAC Address
(xx:xx:xx:xx:xx:xx)
Days of the week
Click to select
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)
Save/Apply

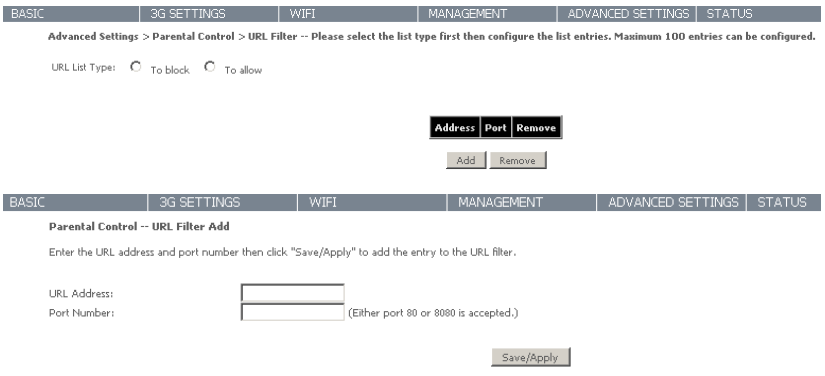
See instructions below and click Apply/Save to apply the settings.

Option	Description
Policy Name	A user-defined label for this restriction
Browser's MAC Address	MAC address of the PC running the browser
Other MAC Address	MAC address of another LAN device
Days of the week	The days the restrictions apply
Start Blocking Time	The time the restrictions start
End Blocking Time	The time the restrictions end

9.4.2 URL filter

With the URL filter, you are able to add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the Connect Router.

Simply check To Block or To Allow and then click Add to enter the URL you wish added to a list



Once you have chosen to add a URL to the list you will be prompted to enter the address. Simply type it in and select Apply/Save.

9.5 Routing

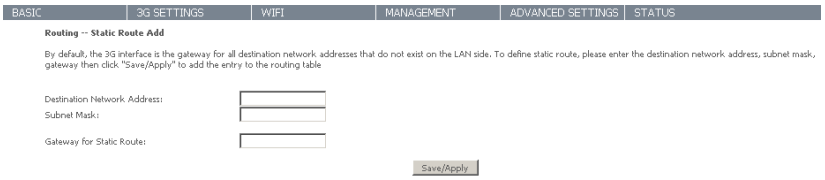
Static Route and Dynamic Route settings can be found in the Routing link.

9.5.1 Static route

The Static Route screen displays the configured static routes.

Click the Add or Remove buttons to change settings.

Click the Add button to display the following screen.

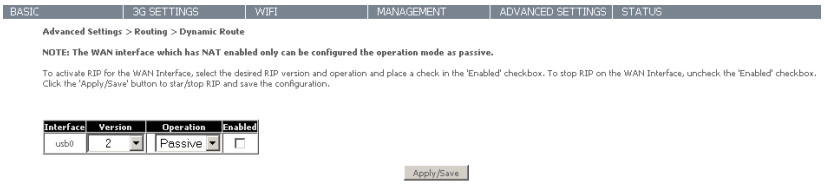

BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Routing -- Static Route Add
By default, the 3G interface is the gateway for all destination network addresses that do not exist on the LAN side. To define static route, please enter the destination network address, subnet mask, gateway then click "Save/Apply" to add the entry to the routing table
Destination Network Address:
Subnet Mask:
Gateway for Static Route:
Save/Apply

Enter Destination Network Address, Subnet Mask. Then click Apply/Save to add the entry to the routing table.

9.5.2 Dynamic route

To activate this option, select the Enabled radio button for Global RIP Mode.

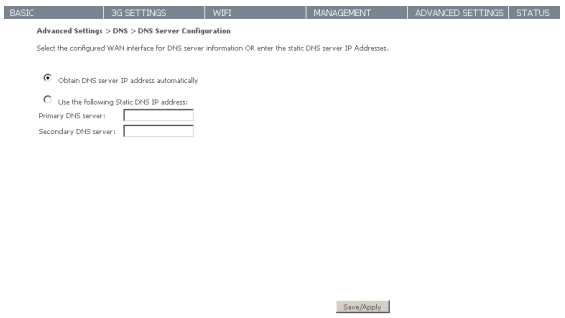
To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the Enabled checkbox for that interface. Click Apply/Save to save the configuration and to start or stop dynamic routing.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Settings > Routing > Dynamic Route
NOTE: The WAN interface which has NAT enabled only can be configured the operation mode as passive.
To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.
Interface
Version
Operation
Enabled
usb0
2
Passive
Apply/Save

9.6 DNS

9.6.1 DNS server

This page allows you to enable automatic DNS from the ISP or specify your own DNS server address manually.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Settings > DNS > DNS Server Configuration
Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses.
Obtain DNS server IP address automatically
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Save/Apply

9.6.2 Dynamic DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of a selection of domains, allowing the router to be more easily accessed from various locations on the Internet.

BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Advanced Settings > DNS > Dynamic DNS
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Router to be more easily accessed from various locations on the Internet.
Choose Add or Remove to configure Dynamic DNS.
Hostname
Username
Service
Interface
Remove
Add
Remove

Note: The Add/Remove buttons will be displayed only if the router has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the Add button and this screen will display.

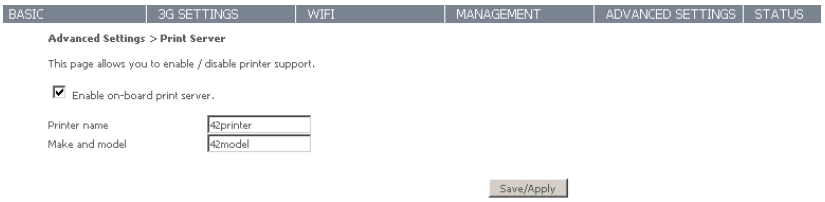
Option	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name for the dynamic DNS server
Interface	Select the interface of the IP address you would like to use from the list
Username	Enter the username for the dynamic DNS server
Password	Enter the password for the dynamic DNS server

9.7 Print Server

This page allows you to enable/disable the USB port of the Connect Router to be used as a print server.

After enabling Print server functionality, you can set your printer name as well as the make and model to provide an easier way to identify the printer.

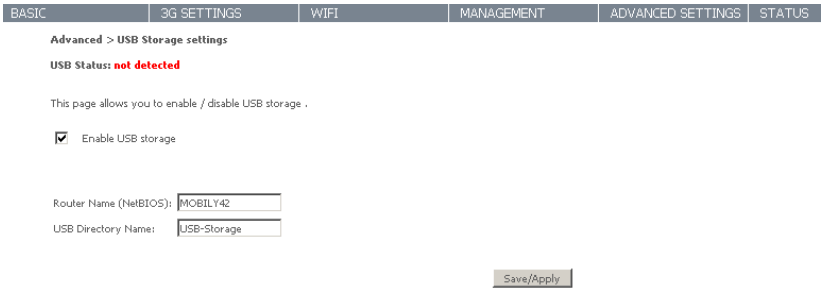
Please see Appendix A for more details on setting up your router to work with Print Server functionality.



9.8 USB Storage

This page allows you to enable/disable the USB port of the Connect Router to be used as a mass storage server.

Please see Appendix B for more details on setting up your router to work with Storage Server functionality.



STATUS

10 Status

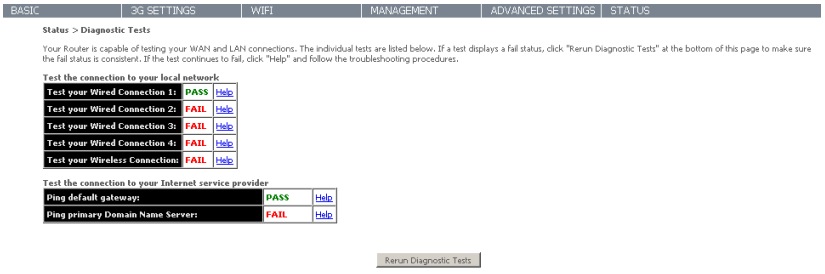
The Status menu has the following submenus:

- Diagnostics
- System Log
- 3G network
- Statistics
- Route
- ARP
- DHCP

10.1 Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status:

1. Click on the Help link
2. Now click Re-run Diagnostic Tests at the bottom of the screen to re-test and confirm the error
3. If the test continues to fail, follow the troubleshooting procedures in the Help screen.

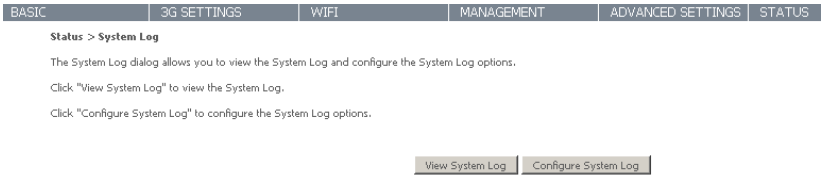

BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Status > Diagnostic Tests
Your Router is capable of testing your WAN and LAN connections. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your Wired Connection 1: PASS Help
Test your Wired Connection 2: FAIL Help
Test your Wired Connection 3: FAIL Help
Test your Wired Connection 4: FAIL Help
Test your Wireless Connection: FAIL Help
Test the connection to your Internet service provider
Ping default gateway: PASS Help
Ping primary Domain Name Server: FAIL Help
Rerun Diagnostic Tests

Option	Description
Test your wired Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of this Router. Fail: Indicates that the Router does not detect the Ethernet interface on your computer.
Test your Wireless Connection	Pass: Indicates that the wireless card is ON. Down: Indicates that the wireless card is OFF.
Ping Default gateway	Pass: Indicates that the Gateway can communicate with the first entry point to the network. It is usually the IP address of the ISP's local Gateway. Fail: Indicates that the Gateway was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	Pass: Indicates that the Router can communicate with the primary Domain Name Server (DNS). Fail: Indicates that the Router was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

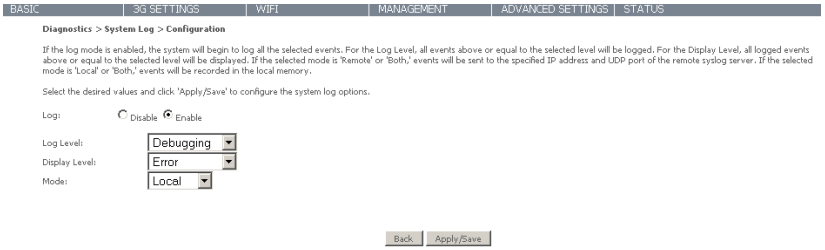
10.2 System Log

This function allows you to view system events and configure related options. Follow the steps below to enable and view the System Log.

1: Click Configure System Log to continue.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Status > System Log
The System Log dialog allows you to view the System Log and configure the System Log options.
Click "View System Log" to view the System Log.
Click "Configure System Log" to configure the System Log options.
View System Log
Configure System Log

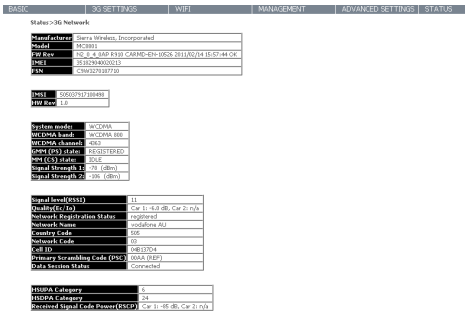
2: Select the system log options (see table below) and click Apply/Save.


BASIC
3G SETTINGS
WIFI
MANAGEMENT
ADVANCED SETTINGS
STATUS
Diagnostics > System Log > Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Apply/Save' to configure the system log options.
Log:
Disable
Enable
Log Level:
Debugging
Display Level:
Error
Mode:
Local
Back
Apply/Save

Option	Description
Log	Indicates whether the system is currently recording events. You can enable or disable event logging. By default, it is disabled.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the Router's SDRAM. When the log buffer is full, the newest event will wrap up to the top of the log buffer and overwrite the oldest event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows you to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, be sent to a remote syslog server, or to both simultaneously. If remote mode is selected, the view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the you to enter the Server IP address and Server UDP port.

10.3 3G Network

Select this option for detailed status information on your Routers 3G connection



Status	Description
Manufacturer	The manufacturer of the embedded 3G module.
Model	The model name of the embedded 3G module
FW Rev	The firmware version of the 3G module.
IMEI	The IMEI (International Mobile Equipment Identity) is a 15 digit number that is used to identify a mobile device on a network.
FSN	Factory Serial Number of the 3G module.
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique 15-digit number used to identify an individual user on a GSM or UMTS network.
HW Rev.	The hardware version of the 3G module.
Temperature	The temperature of the 3G module in degrees Celsius.
System Mode	WCDMA/Europe CDMA 2000 / America
WCDMA band	The 3G radio frequency band which supports tri-band UTMS/HSDPA/HSUPA frequencies (850/1900/2100 MHz), IMT2000 is 2100 MHz, WCDMA800 is 850 MHz, WCDMA1900 is 1900 MHz.
WCDMA channel	The 3G channel.
GSM channel	The 2G channel.
GMM (PS) state	Packet Switching state
MM (CS) state	Circuit Switching state
Signal Strength 1	The 3G/2G service signal strength in dBm.
Signal Strength 2	The 3G/2G service signal strength in dBm.

10.4 Statistics

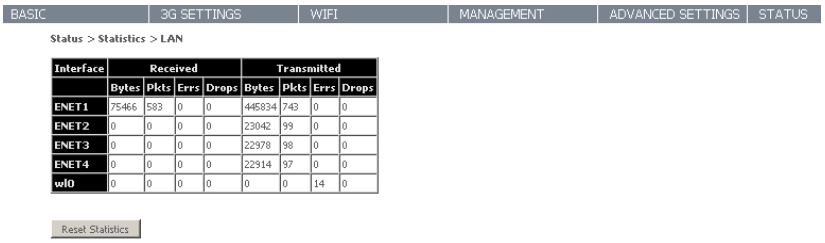
These screens provide detailed information for the:

- Local Area Network (LAN)
- 3G Interfaces

NOTE: These statistics page refresh every 15 seconds.

10.4.1 LAN

This screen displays statistics for the Ethernet and Wireless LAN interfaces



Interface	Shows connection interfaces	
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

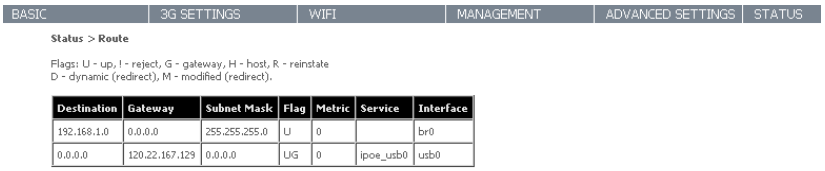
10.4.2 3G Network

This page displays the inbound and outbound statistics of the 3G network

Interface	Shows connection interfaces	
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

10.5 Route

Select Route to display the network routes configured on the Router has found.



10.6 ARP

Click ARP to display the ARP information.

10.7 DHCP

Click DHCP to display the DHCP information.

10.8 PING

Check a connection by entering the IP address

Appendix

11 Appendix A: Print Server

These steps explain the procedure for enabling the Print Server.

1. Select “Print Server” from the Advanced Settings menu in the Web User Interface.

Select the Enable on-board print server checkbox and enter the Printer name and the Make/ model

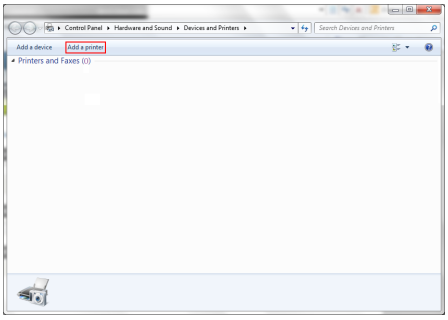
NOTE: The Printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.

11.1 For Windows Vista/7

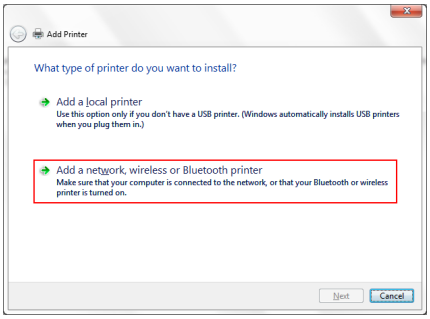
These steps explain the procedure for enabling the Printer Server.

1. Go to the control panel, and select ‘Printers’ if you are using Windows Vista or select “Devices and Printers” if you are using Windows 7.

Once in the ‘Printers’ page, click the ‘Add a printer’ button as shown below.

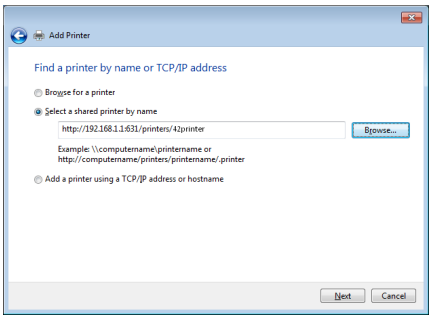


2. Select ‘Add a network, wireless or bluetooth printer’

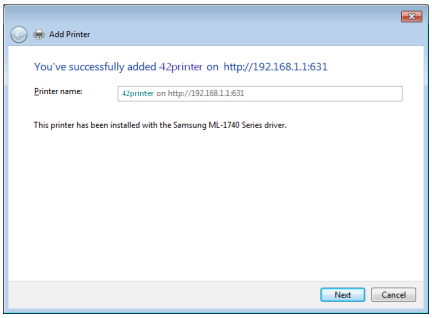

Add Printer
What type of printer do you want to install?
Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)
Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.
Next
Cancel

3. Click on the radio-button labelled 'Select a shared printer by name', and type "http://192.168.1.1:631/printers/42printer" in the box below. Click 'Next'.

NOTE: The PrinterName must be the same as the printer name entered into the Printer section of Connect Router's user interface.



4. Next, select the driver that came with your printer. Browse through the list to select your printer driver, or click 'Have Disk' if you have your printer driver installation media.
5. Choose whether you want this printer to be the default printer, and then click 'Next'.

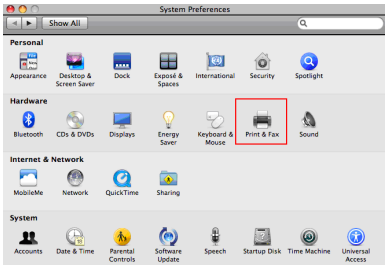


6. Click 'Finish'. Your device is now configured and ready for use.

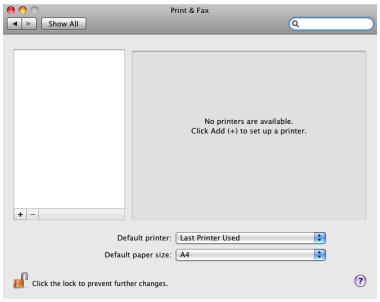
11.2 For MAC OSX

These steps explain the procedure for enabling the Printer Server.

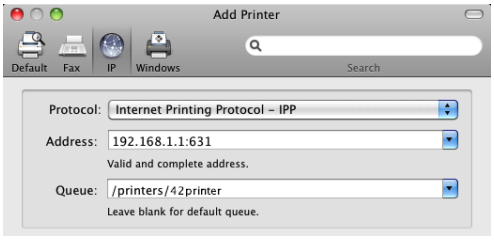
1. Click on the Apple menu, select System Preferences.
2. In the System Preference menu click on the Print & Fax.



3. Click the + button to add your printer.

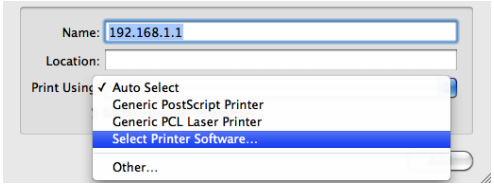


4. Mouseover to the Protocol drop down list and select Internet Printing Protocol – IPP
5. In the Address field, type “192.168.1.1:631”
6. In the Queue field, type “/printers/{PrinterName}”

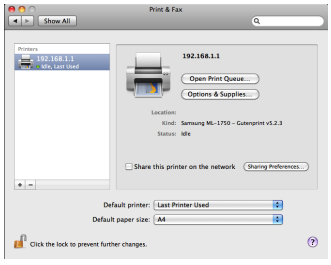


NOTE: {PrinterName} must be the same as the printer name entered into the Printer section of the Connect Router’s user interface.

7. From the Print Using drop down list, select your corresponding printer driver.



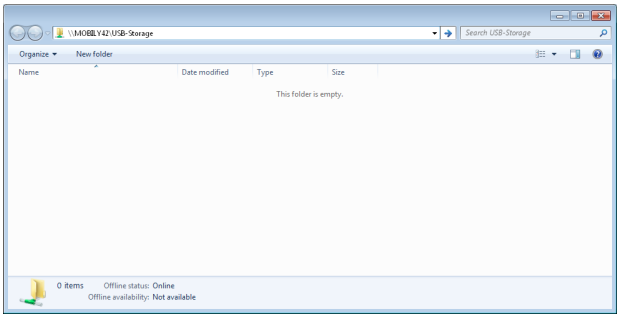
8. Click Add and check the printer status.



12 Appendix B: Samba Server

12.1 For Windows Vista/7

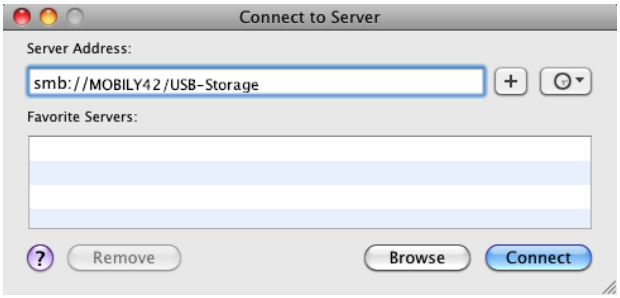
1. Open a web-browser (such as internet Explorer, Firefox or Safari)
2. Type in the address \\ “NetbiosName”\ “DirectoryName” \ (eg \\MOBILY42 \USB-Storage)



Note: There are no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive.13.2 For MAC OSX

12.2 For MAC OSX

1. Click the finder icon in the Dock.
2. Choose Connect to Server from the Go menu.
3. In the address field of the Connect to Server dialog, type in the URL Smb:// “NetbiosName”/“DirectioryName” (eg Smb:// MOBILY42/USB-Storage))



4. Select Connect to connect your USB driver.

user manual

mobily... my world, my choice

customer service: 056-010-1100 | www.mobily.com.sa